HISOLUTIONS

Gesetzeslage aktuell

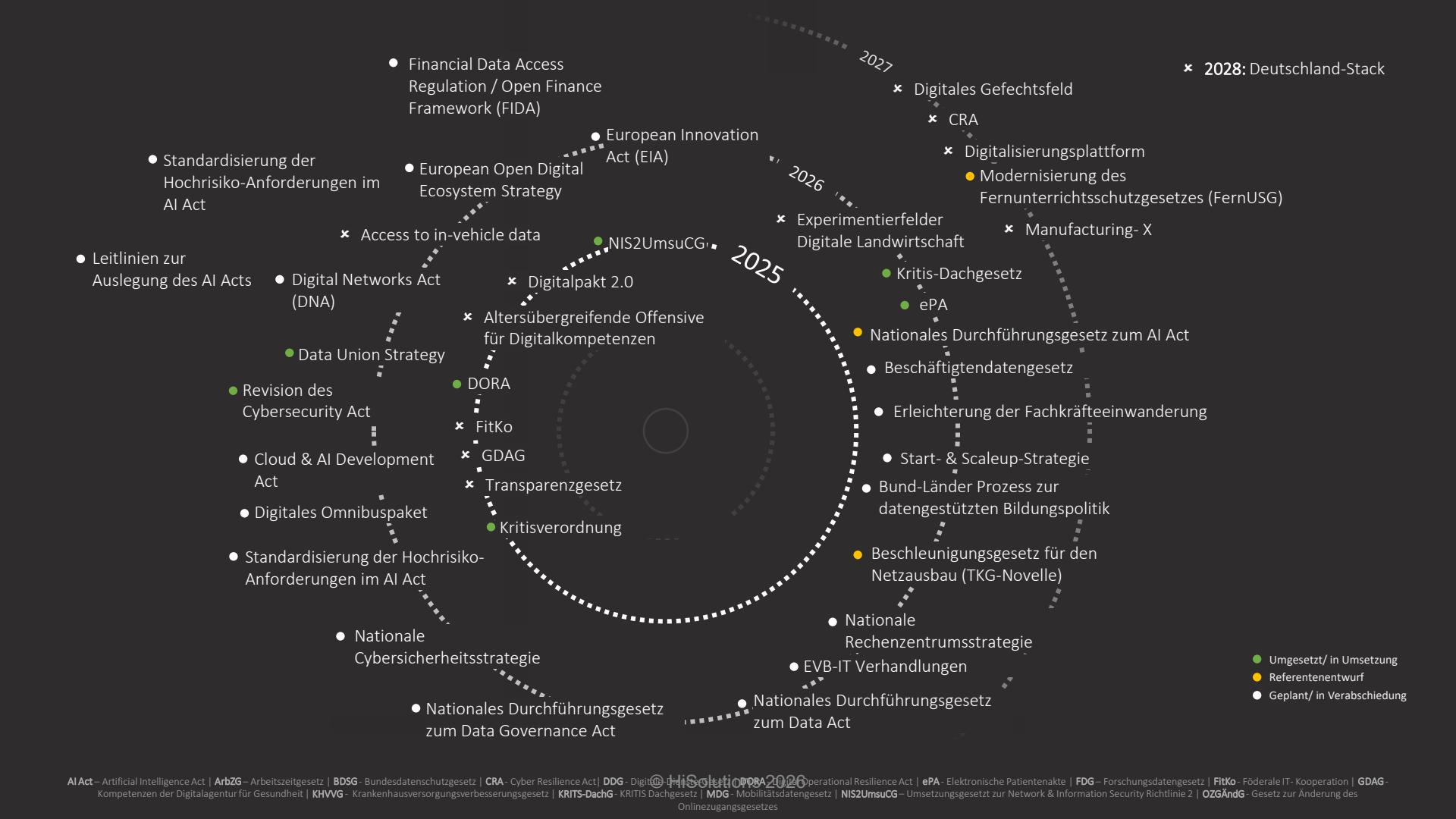
mit Lösungsansätzen

Know-how to go | 10. Juni 2026

Manuel HonkHase Atug

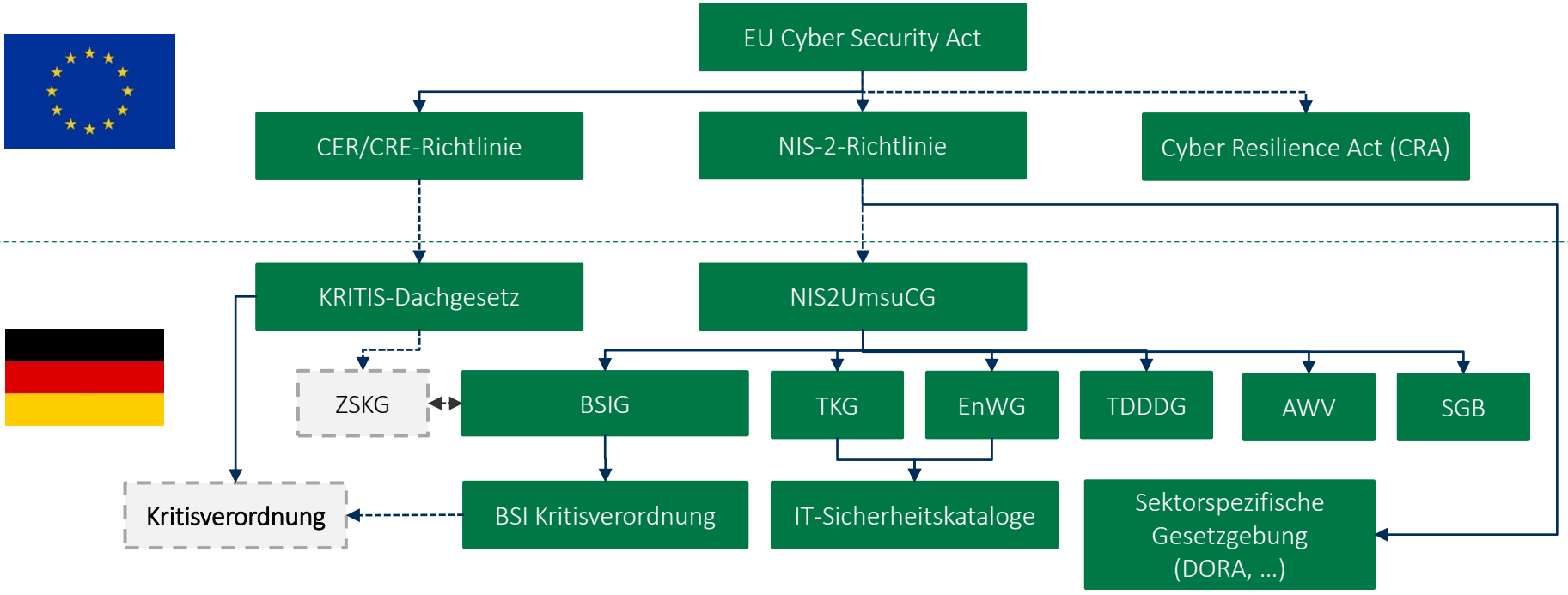
Resilienz durch Security!

→ Denn Security sichert das Business ab



AI Act – Artificial Intelligence Act | **ArbZG** – Arbeitszeitgesetz | **BDSG** - Bundesdatenschutzgesetz | **CRA** - Cyber Resilience Act | **DDG** - Digitale-Dienste-Gesetz | **DORA** - Digital Operational Resilience Act | **ePA** - Elektronische Patientenakte | **FDG** – Forschungsdatengesetz | **FitKo** - Föderale IT- Kooperation | **GDAG** - Kompetenzen der Digitalagentur für Gesundheit | **KHVVG** - Krankenhausversorgungsverbesserungsgesetz | **KRITS-DachG** - KRITIS Dachgesetz | **MDG** - Mobilitätsdatengesetz | **NIS2UmsuCG** – Umsetzungsgesetzt zur Network & Information Security Richtlinie 2 | **OZGÄndG** - Gesetz zur Änderung des Onlinezugangsgesetzes

Übersicht zur Regulierungsstruktur



Grün: verabschiedet **Grau**: In Arbeit

Kritisverordnung: Referentenentwurf

Aus der BSI-Kritisverordnung wird die Kritisverordnung

- Mit der Verordnung werden die Vorgaben aus § 4 Abs. 3 und § 5 Abs. 1 KRTISDachG umgesetzt
- Vorgaben für KRITIS-Sektoren und -Branchen aus der europäischen "Delegierten Verordnung (EU) 2023/2450" integriert
- Neuer KRITIS-Sektor Weltraum
- Die in der Verordnung genannten Schwellenwerte basieren weiter auf einem Regelschwellenwert von 500.000 zu versorgenden Einwohnern
- Nach dem Inkrafttreten gültig für Kritis-Dachgesetz und BSI-Gesetz

Quellen:

Kritisverordnung RefE:
https://ag.kritis.info/2026/05/28/referentenentwurf-des-bmi-verordnung-zur-bestimmung-kritischer-anlagen-nach-dem-kritis-dachgesetz-kritisverordnung-kritisv/

EU DVO 2023/2450:
https://eur-lex.europa.eu/eli/reg_del/2023/2450/oj/deu

EU NIS-2, NIS2UmsuCG & BSI-Gesetz (BSIG)

NIS-2-Pflichten

§ 33, § 34 Registrierungspflicht
- Bestimmung der eigenen Betroffenheit und Registrierung bei zuständiger Behörde (BSI, BBK, BNetzA oder BaFin)

§ 30, § 31 Risikomanagement inkl. technischer und organisatorischer Maßnahmen
- Umsetzung geeigneter, verhältnismäßiger, wirksamer, auf Stand der Technik sowie Standards/Normen und Risikoexposition basierender TOM

§ 32 Meldemechanismen inkl. Unterrichtungspflicht
- Vorgehen im Krisenfall, Identifikation von internen und externen Ansprechpartnern, interne Sicherheitsvorfalldefinition und -behandlung

§ 39 Nachweispflicht
- über Risikomanagement, Einhaltung der Meldepflichten und Systeme zur Angriffserkennung, z. B. über Auditergebnisse, Prüfungen oder Zertifikate

§ 38 Geschäftsleitungspflichten
- Umsetzung und Überwachung des Risikomanagements, Schulungspflicht für C-Ebene zu Risikomanagement und Sicherheit in der IT

kurz gesagt

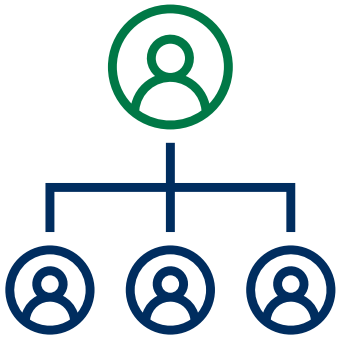
- Umfassende Anforderungen zur Informationssicherheit
- Ca. 30.000 Unternehmen betroffen
- Inklusion der Lieferkette
- Wenige Ausnahmen (in der Wirtschaft)
- Befugniserweiterung für das BSI
- Empfindliche Strafen

Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen

- **Geschäftsleitungen besonders wichtiger Einrichtungen** und **wichtiger Einrichtungen** sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden **Risikomanagement-maßnahmen umzusetzen** und **ihre Umsetzung zu überwachen**.

- Die **Geschäftsleitungen besonders wichtiger Einrichtungen** und **wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen**, um ausreichende Kenntnisse und Fähigkeiten zur **Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken** im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die **Auswirkungen von Risiken sowie Risikomanagementpraktiken** auf die von der Einrichtung erbrachten Dienste beurteilen zu können.

Kurz gesagt



Geschäftsleitungen

steuern, *delegieren,*

überwachen und *kontrollieren*

1. Paper Compliance
2. Prozessgestaltung & -implementierung
3. Prozessüberprüfung (Vollständigkeit)
4. Wirksamkeitsprüfung (aller Prozesse)

Cybersicherheit: Risikomanagement

Umsetzung von **angemessenen** und **verhältnismäßigen** Maßnahmen in verschiedenen Themenbereichen

Kriterien

- Risikoexposition
- Größe der Einrichtung
- Umsetzungskosten
- Eintrittswahrscheinlichkeit
- Schwere von Sicherheitsvorfällen
- Gesellschaftliche/wirtschaftliche Auswirkungen

Themenbereiche

- Risiko-Management
- Informationssicherheitsmanagement
- Asset Management
- Technische Sicherheit
- Personelle & organisatorische Sicherheit
- Notfall- & Krisen-Management
- Lieferanten, Dienstleister und Dritte
- Vorfallerkennung und -bearbeitung

KRITIS: Maßnahmen sind verhältnismäßig, wenn der erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage steht.

Kritis-Dachgesetz (KRITISDachG)

Kurzeinordnung EU-CER

- Europäische Richtlinie (EU) 2022/2557 über ***C**ritical **E**ntities **R**esilience (CER)*
- Nationale Umsetzung in Deutschland durch das KRITIS-Dachgesetz (KRITIS-DachG) seit 17. März 2026
- Ergänzt bestehende Vorgaben aus dem IT-Sicherheitsrecht (z. B. NIS-2, BSIG)
- Fokus auf der Resilienz kritischer Einrichtungen und dem Schutz physischer Infrastrukturen

Verhinderung von Sicherheitsvorfällen durch wirksame Resilienzmaßnahmen unter Berücksichtigung von Katastrophenvorsorge und Anpassung an den Klimawandel

Schwerpunkte des KRITIS-Dachgesetzes

- Umsetzung eines All-Gefahren-Ansatzes zur Berücksichtigung natürlicher, technischer, gesundheitlicher und menschlich verursachter Risiken
- Verpflichtung zur Durchführung von Risikoanalysen und Erstellung von Resilienzplänen
- Aufbau und Pflege wirksamer Strukturen für das Krisen- und Notfallmanagement
- Schulung und Sensibilisierung von Leitung und Personal

Das KRITIS-Dachgesetz erweitert den Fokus von der IT-Sicherheit hin zum Schutz physischer Infrastrukturen

KritisDG - physische Sicherheit

- Alle 4 Jahre: Risikoanalysen und -bewertungen!

„Wirtschafsstabilität beeinträchtigende, ***naturbedingte****,* ***klimatische*** *und vom Menschen verursachte Risiken berücksichtigen, darunter solche* ***sektorübergreifender oder grenzüberschreitender Art****,* ***Unfälle****,* ***Naturkatastrophen****,* ***gesundheitliche Notlagen****, sowie* ***hybride Bedrohungen*** *oder andere* ***feindliche Bedrohungen****, einschließlich* ***terroristischer Straftaten****“ sowie „Wirtschafsstabilität beeinträchtigende Risiken berücksichtigen, die sich aus dem* ***Ausmaß der Abhängigkeiten anderer Sektoren*** *von der kritischen Dienstleistung ergeben, die von der kritischen Anlage –* ***auch in benachbarten Mitgliedstaaten und Drittstaaten*** *– erbracht wird“*

- Alle 2 Jahre: Resilienzplan nachweisen!

Anforderungen nach dem KRITIS-Dachgesetz

Risikoanalyse & Bewertung

Ermittlung und Bewertung von Risiken nach dem risikobasierten All-Gefahren-Ansatz (Natur, Technik, Mensch) zur Vorbereitung auf Not- und Krisenfälle

Durchführung von Schulungen und Übungen

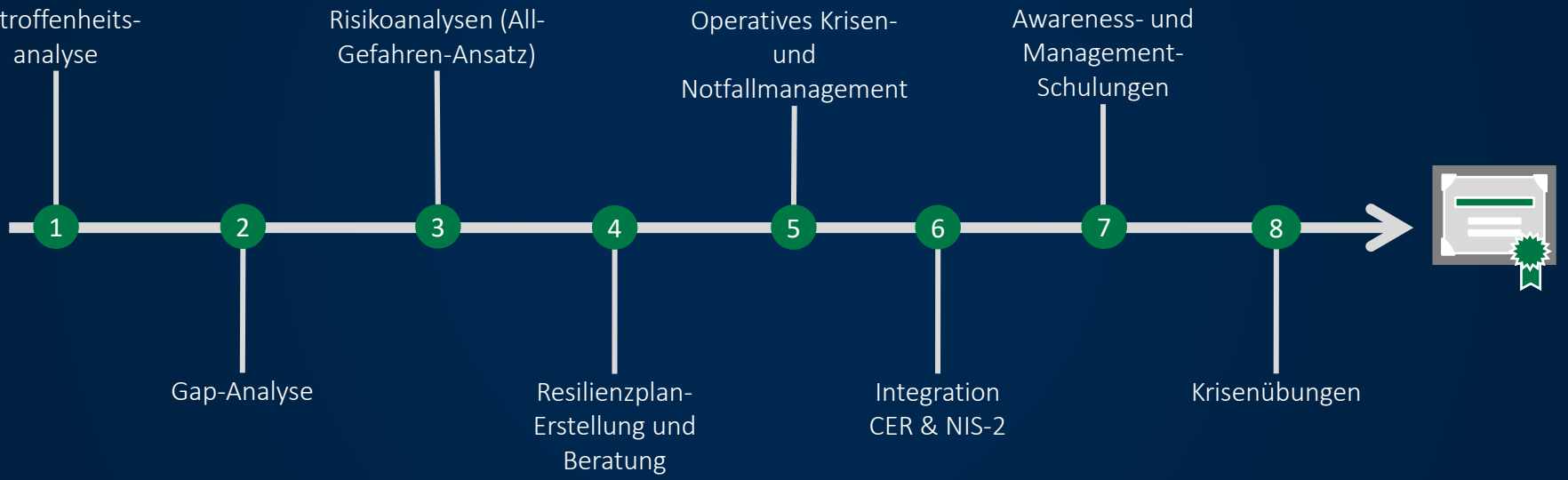
Regelmäßige Trainings zur Stärkung der Resilienz sowie Tests und Krisenübungen zur Vorbereitung auf Not- und Krisenfälle

Resilienzplanung & Maßnahmen

Definition und Dokumentation von Präventions-, Reaktions-, Wiederanlauf- und Personalsicherheitsmaßnahmen

Krisenmanagement & Kommunikation

Aufbau und Pflege von Rollen, Meldewegen und Kommunikationsstrukturen zur Bewältigung von Krisen

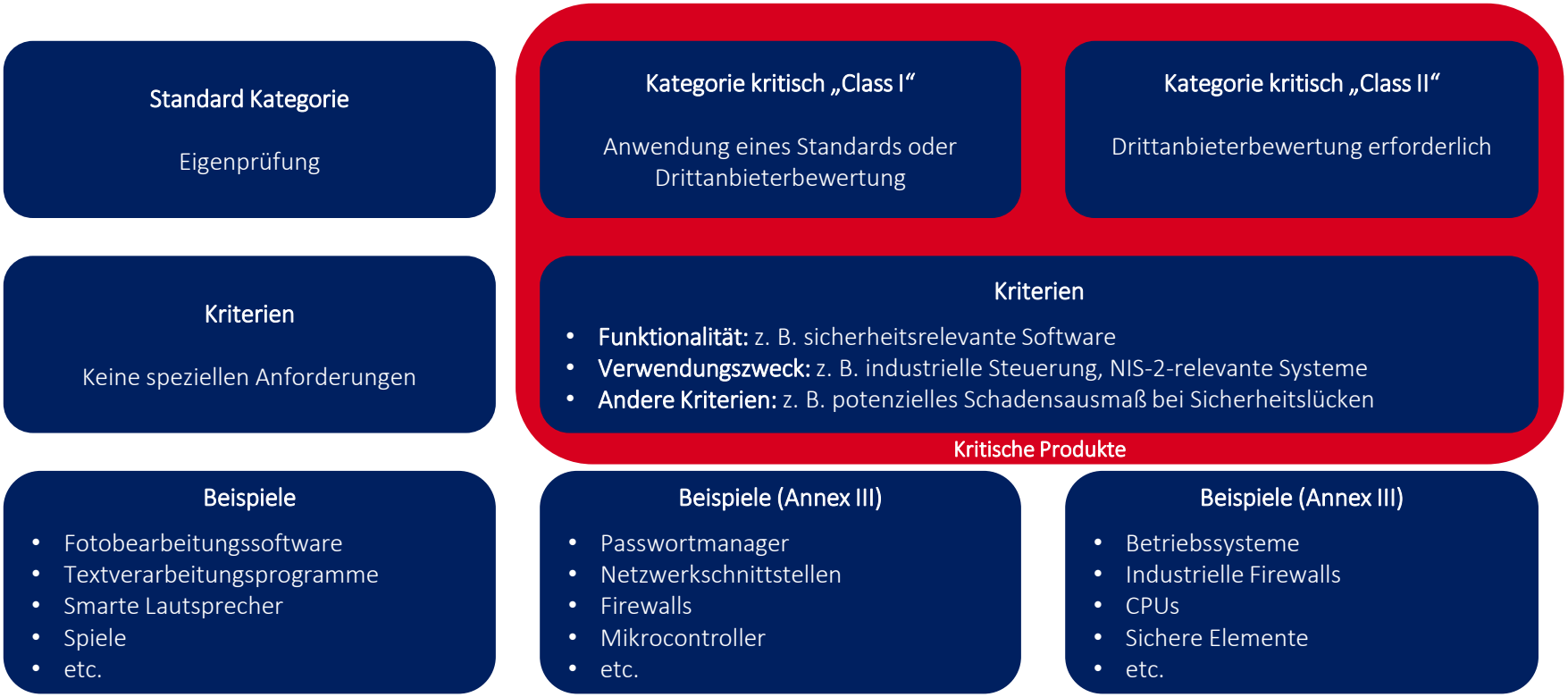


Cyber Resilience Act (CRA)

Was ist der Cyber Resilience Act (CRA)?

- **EU-weite Cybersicherheitsstandards** für digitale Produkte (Hardware & Software) zur Stärkung der digitalen Sicherheit
- **Pflichten für Hersteller:** Sicherheitskonzepte wie „Security by Design“ und regelmäßige Updates über den gesamten Produktlebenszyklus
- **Transparenz & Meldepflicht:** Software-Stückliste (SBOM) und Meldung von Sicherheitsvorfällen innerhalb von 24 Stunden
- **Umsetzung & Sanktionen:** Inkrafttreten seit Dez. 2024, vollständige Anwendung bis Dez. 2027; bei Verstößen drohen Geldstrafen und Verkaufsverbote

Wie der Cyber Resilience Act in der Praxis funktioniert



Post Quanten Crypto (PQC)

Harvest Now, Decrypt Later

Daten sammeln → Auf QC warten → Ent-schlüsseln

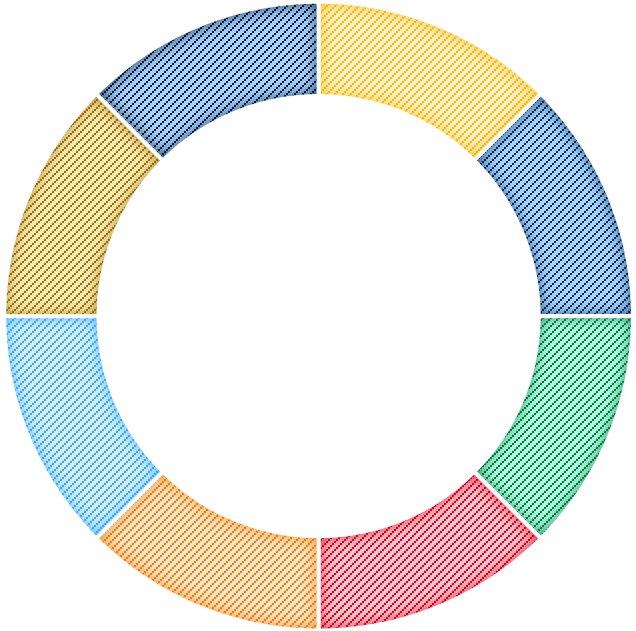
Staatliche Akteure sammeln bereits heute viele verschlüsselte Daten

Je länger Daten vertraulich bleiben müssen, desto dringender ist der Handlungsbedarf

Kryptografie ist ein Querschnittsthema

Eine PQC-Migration lässt sich nicht an die IT delegieren

Sie erfordert Kooperation über alle Bereiche und ist damit eine Management-Aufgabe



Zeitstrahl der PQC-Migration innerhalb der Europäischen Union[1]

15.12.2025
BSI beginnt bei Behörden, Kryptokataster abzufragen

Wahrscheinlichster Zeitpunkt, ab dem State Actors Zugang zu krypto-relevanten Quanten-computern haben werden

2025 | 2026 | 2027 | 2028 | 2029 | 2030

31.12.2026
EU empfiehlt, erste Schritte zu implementieren

→ z. B. Kryptokataster

31.12.2030
Klassische Public-Key-Kryptografie veraltet; Quantum-sicher sollte der Standard sein

[1] EU Roadmap for the Transition to Post-Quantum Cryptography

Technologische Entwicklungen erfordern einen neuen Umgang mit Kryptografie – auch in der Informationssicherheit

Kryptografische Verfahren werden dynamisch – von einem statischen Bestandteil hin zu einem aktiv verwalteten Asset

Das Ergebnis: Krypto-Agilität

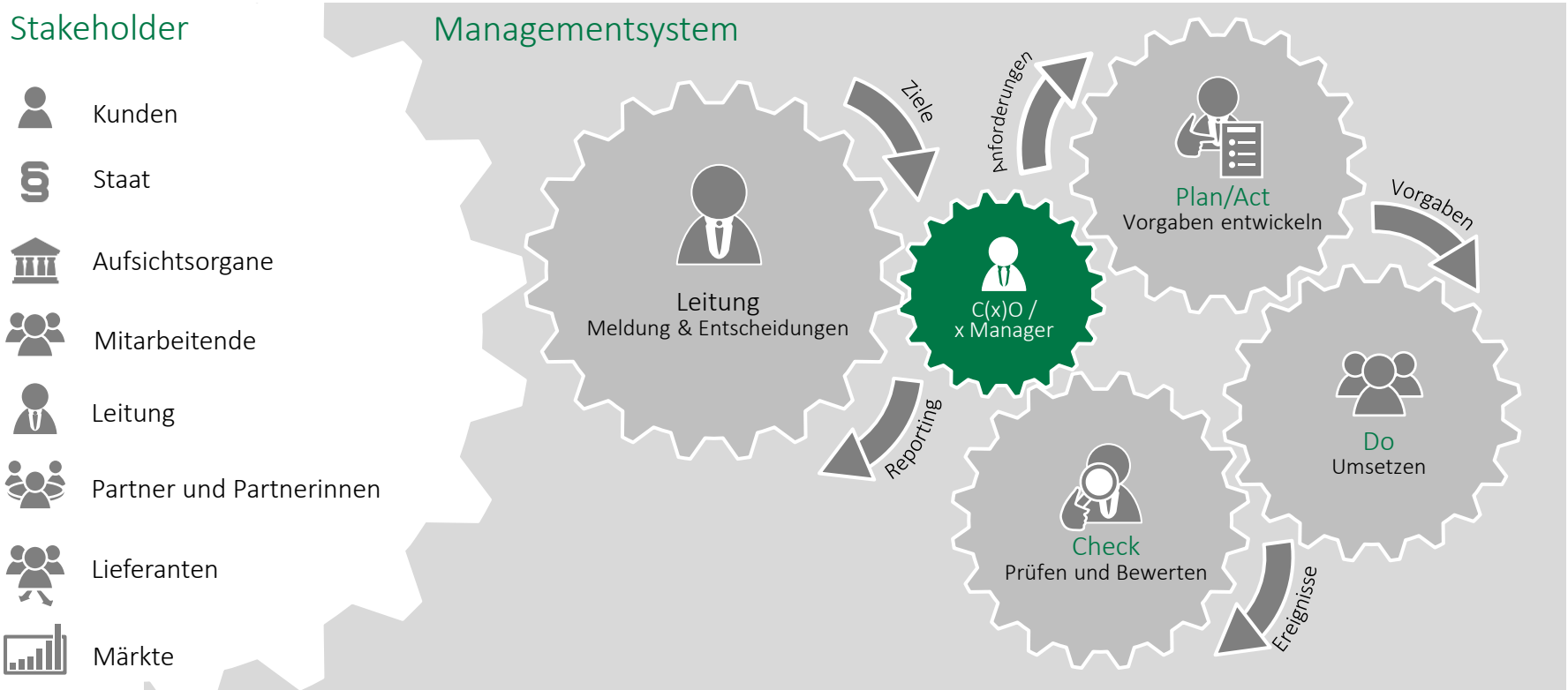
1. Quantencomputer neutralisieren einen Großteil bisheriger Maßnahmen zum Schutz von Informationen
2. Regulierungsbehörden empfehlen eine Migration
3. PQC wird zum Stand der Technik

→ Die Migration zu quantensicheren Systemen ist keine einmalige Aufgabe
→ PQC erfordert kontinuierliche Überwachung der eingesetzten Kryptografie, technische Anpassungen und regulatorische Nachsteuerung

„PQC wird massiv unterschätzt. Es erfordert einen grundlegend anderen Umgang mit Kryptografie und ist komplex. Die Umsetzung braucht Zeit und strategische Planung, um nachhaltig zu wirken.“

ISMS vs. Integriertes Managementsystem (IMS)

Allgemeiner Aufbau eines Managementsystems

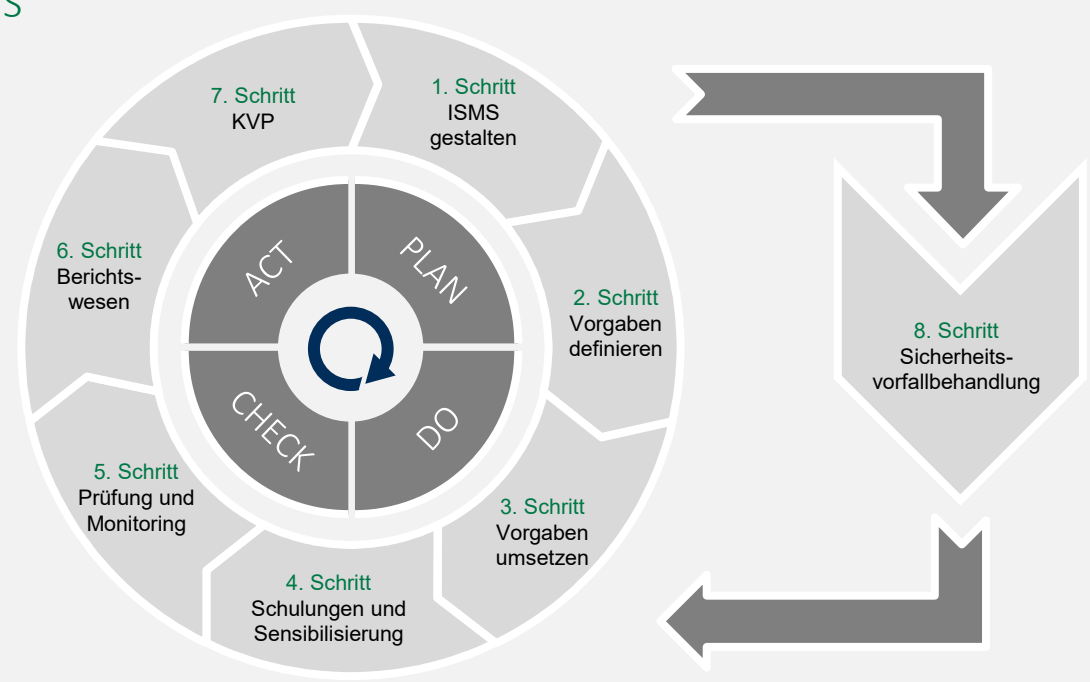


Klassisches Informationssicherheitsmanagement (ISMS)

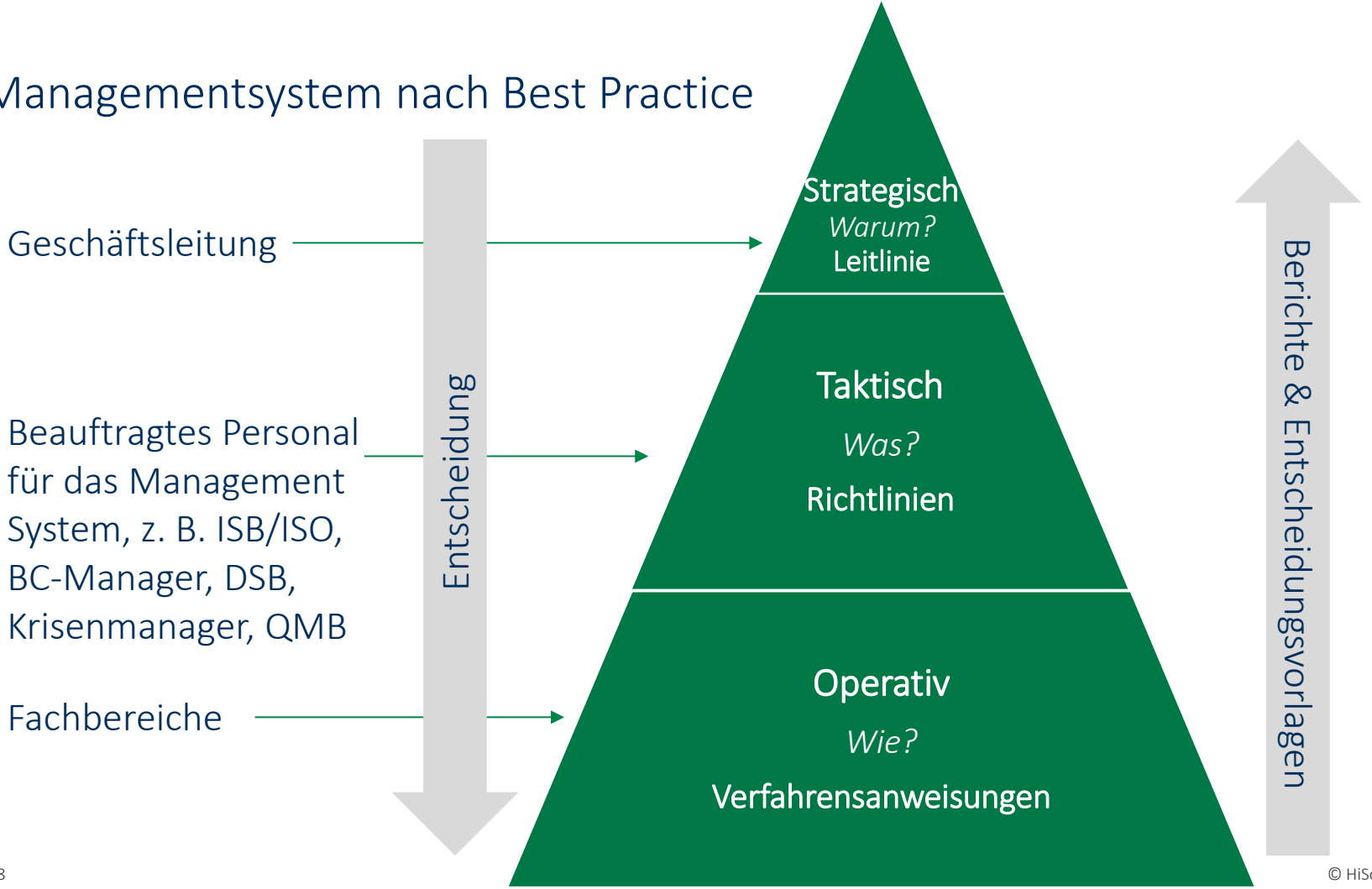
ISMS-Anforderungen

- Gesetzliche Vorgaben
- Externe Vorgaben
- Konzernanforderungen
- Unternehmensziele
- Interne Anforderungen

ISMS

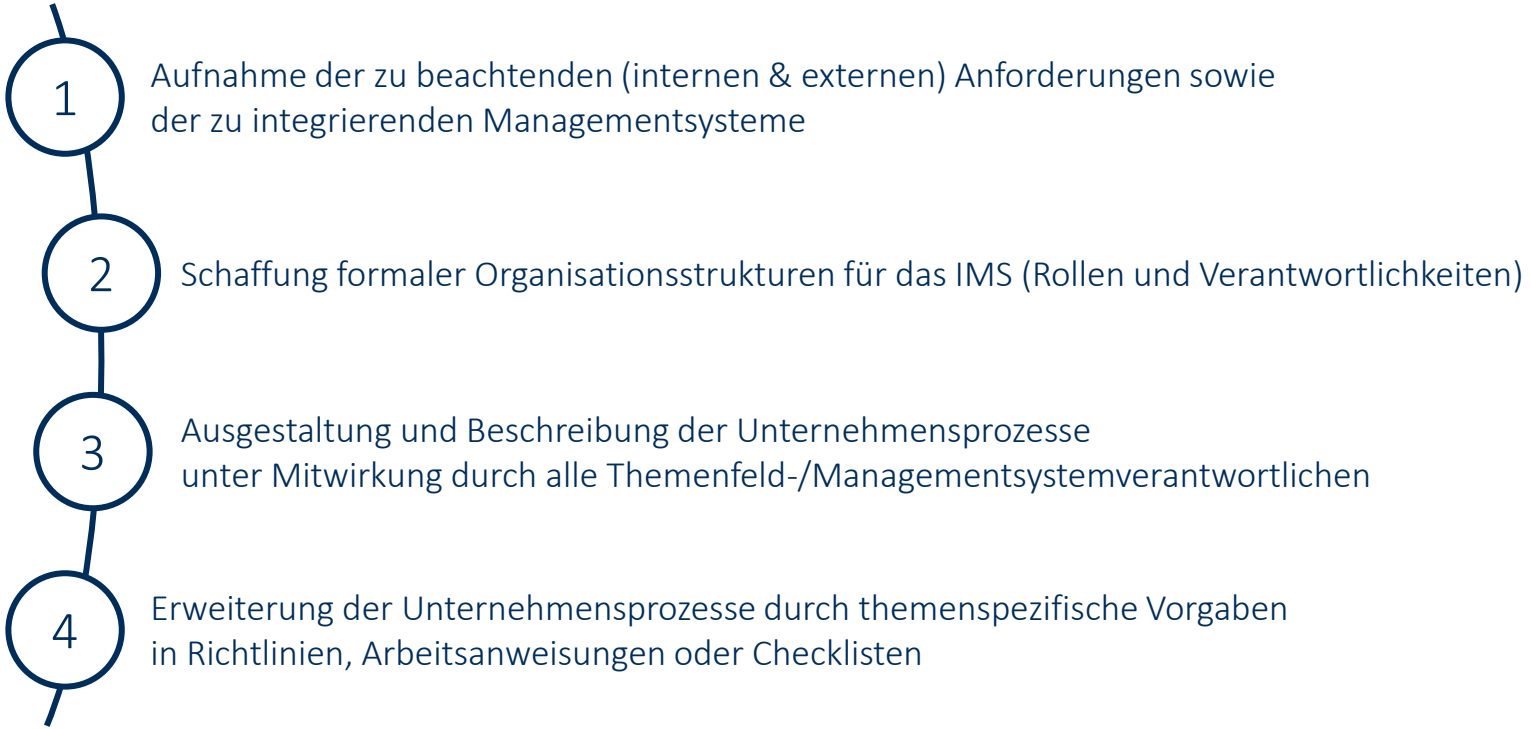


Managementsystem nach Best Practice



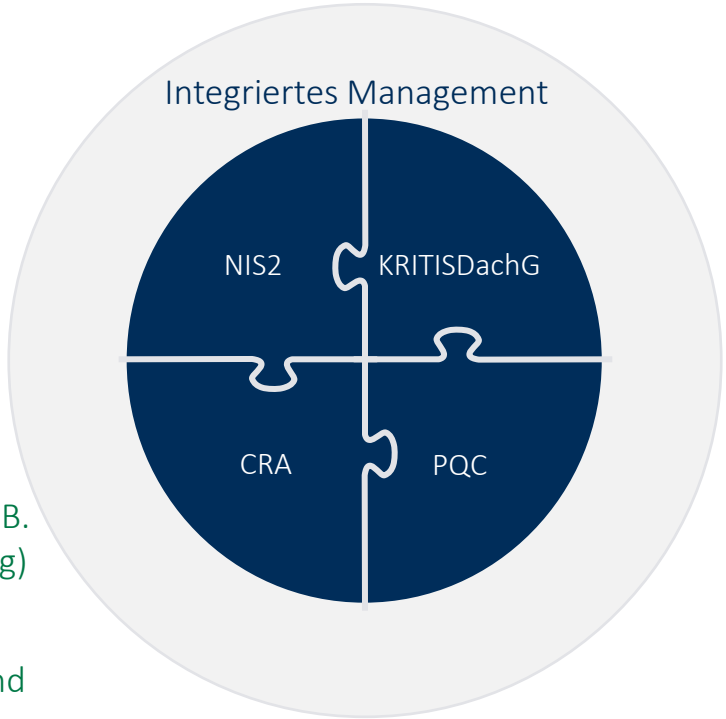
Strukturierte Vorgehensweise der Implementierung

Umsetzung eines IMS



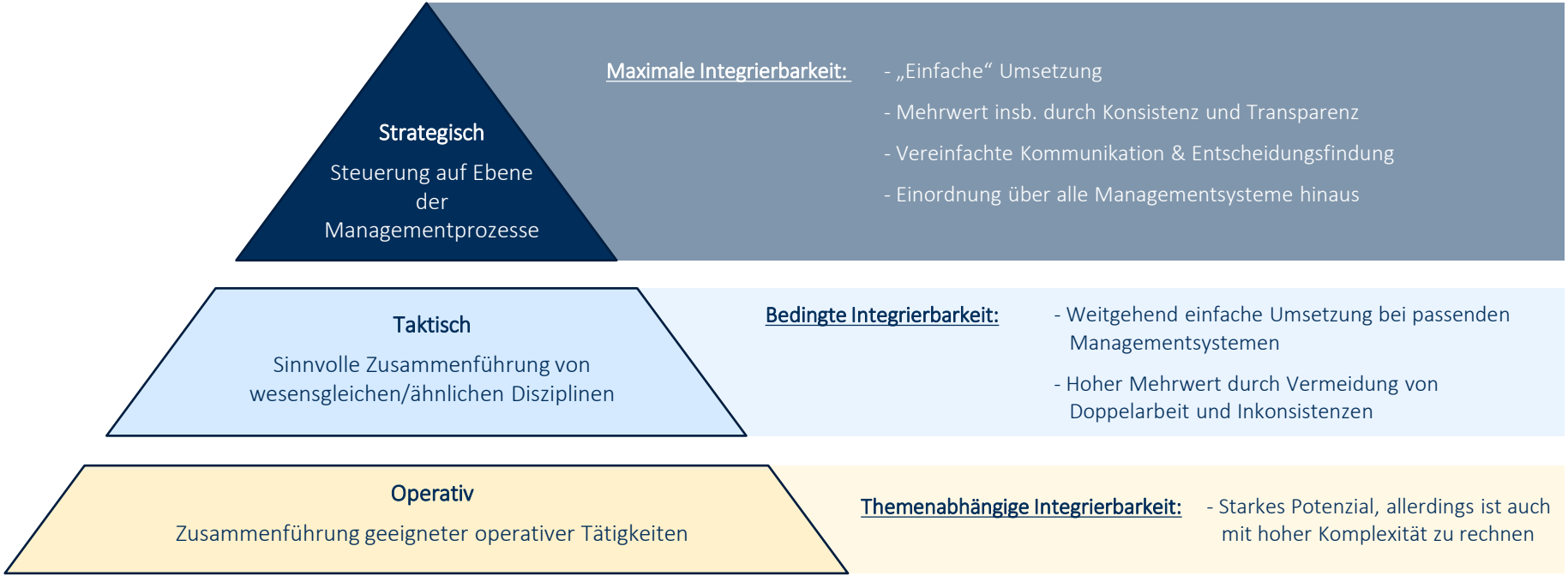
Ein Integriertes Managementsystem vereint eine Vielzahl von Vorteilen

- Gemeinsame Organisationsstrukturen
- Schlankes und ressourcenschonendes Management
- Reduzierung von Kosten
- Nutzung von Synergien (z. B. Schulung & Sensibilisierung)
- Einheitliches Reporting und Management Reviews

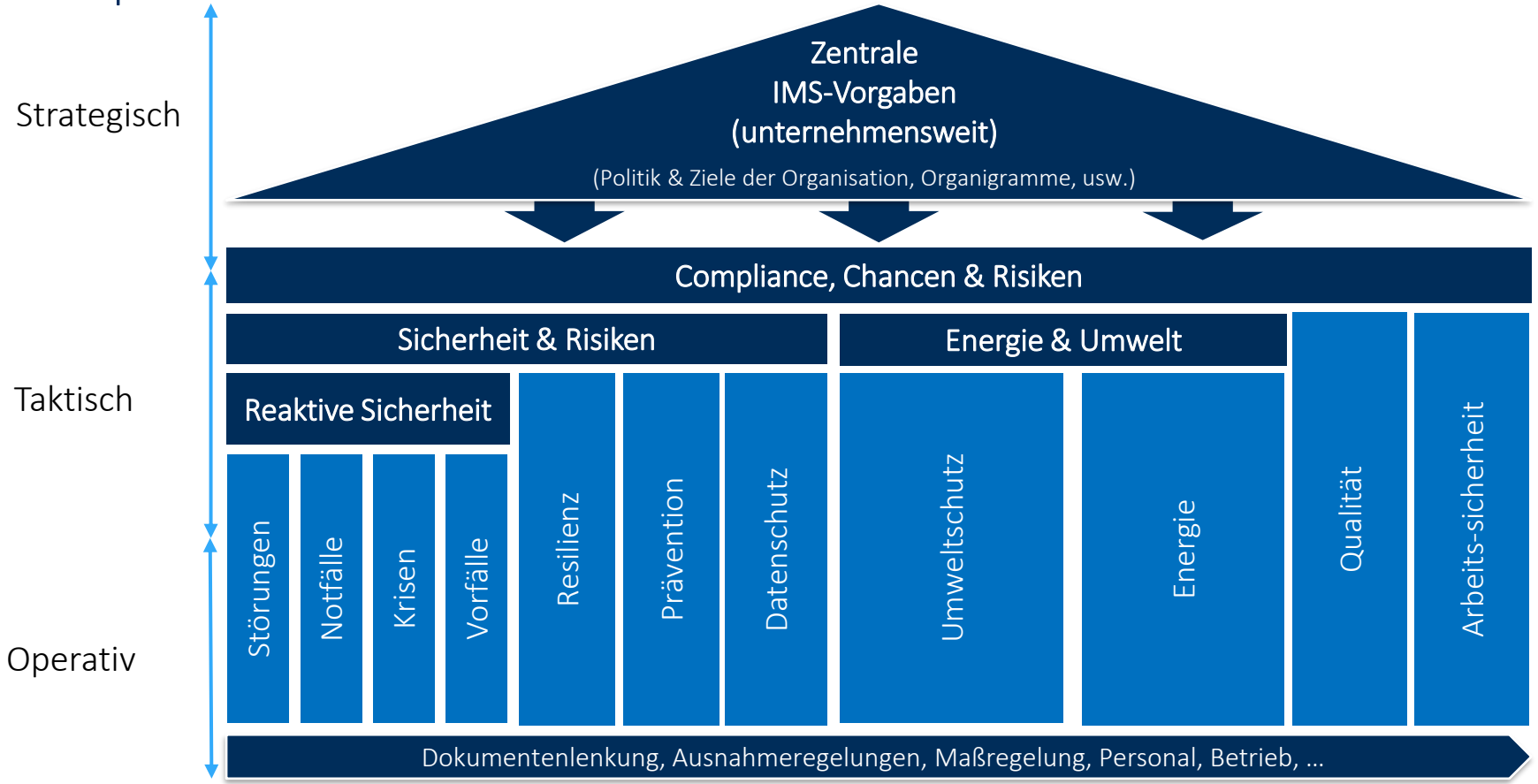


- Geringerer Dokumentationsauswand
- Einheitliche Begriffe und Definitionen
- Möglichkeit der gemeinsamen Zertifizierung
- Vermeidung von Doppelaufwänden
- Zentrales Risikomanagement

Integrierbarkeit von unterschiedlichen Managementsystemen



Beispielhafter Aufbau eines IMS



Kontakt

Manuel Atug

Principal